UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,928	03/31/2000	Ulhas S Warrier	10559-148001/P7973	2224

20985 7590 12/01/2004

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/539,928	WARRIER ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1, 2, 3, 6- 23, and 25-34* is/are pending in the application.

4a) Of the above claim(s) *4,5 and 24* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 3, 6- 23, and 25-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 23 September 2004 in which a Request for Continued Examination (RCE) was submitted in response to Final Rejection sent 14 May 2004, with an original application filed 31 March 2000.

2. Claims 1, 2, 3, 6-23, 25-34 are currently pending in this application. Claims 1, 9, 17, 21, and 30 are independent claims. Claims 4, 5, and 24 have been withdrawn. Claims 30-34 are new. Claims 25, is currently amended.

Response to Arguments

3. Applicant's arguments filed 23 September 2004 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 1, 7, 9, 10, 13 and 17** are rejected under 35 U.S.C. 102(e) as being anticipated by Harrison et al. U.S. Patent No. 6,539,483 (hereinafter '483).

As to independent claim 1, "A method of managing a network session comprising" is taught in '483 col. 3, lines 29-43;

"delivering security policies from a server to a remote system that has predetermined configuration information and allows running at least one application

program; establishing a secure virtual private network connection between the server and the system" is shown in '483 col. 5, lines 23-62;

"regulating activities in the system based on both of the security policies and a context of said at least one application program including at least a state of running of said at least one application program" is disclosed in '483 col. 4, lines 43-60.

As to dependent claim 7, "further comprising updating the set of policies" is taught in 483 col. 5, lines 48-50.

As to independent claim 9, this claim is directed to a computer-readable medium of the method of claim 1 and is rejected along similar rationale.

As to dependent claims 10, this claim contains substantially similar subject matter as claim 7; therefore it is rejected along the same rationale.

As to dependent claim 13, "wherein the rejection criteria includes the set of policies" is taught in '483 col. 3, lines 29-33.

As to independent claim 17, this claim is directed to the system of the method of claim 1 and is rejected along similar rationale.

6. **Claims 21, 22, and 23,** are rejected under 35 U.S.C. 102(e) as being anticipated by of Naveh et al., U.S. Patent No. 6,466,984 (hereinafter '984).

As to independent claim 21, "A network stack comprising: a policy engine a policy store adapted to interact with the policy engine and store a set of policies from the policy engine;" is taught in '984 col. 7 lines 16-60;

"a socket interceptor coupled to the policy engine; a packet guard coupled to the policy engine" is shown in '984 col. 7, line 60 through col. 8, line 7;

"a configurable management process adapted to reconfigure the network stack and having instructions to: receive policies in the policy engine from the policy server" is disclosed in '984 col. 9, lines 18-55

"use the socket interceptor to detect and reject data packets from unauthorized users and applications and provide the packet guard with context information about the unauthorized users and applications including at least information about a running state of the application" is taught in '984 col. 13, lines 27-53;

"use the packet guard to filter unauthorized activities received from the network interface; use the packet guard to filter the data packets from unauthorized users and applications based on the context information received by the socket interceptor; and use the packet guard to filter data packets based on the policies and provide the packet guard with context information about the unauthorized users and applications including at least information about a running state of the application" is shown in col. 15, lines 15-55.

As to dependent claim 22, "The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard" is shown in '984 col. 7, lines 16-60.

As to dependent claim 23, "The network stack of claim 21 further comprising an interface to a network adapted to connect the network stack to the network, wherein the network has a policy server" is disclosed in '984 col. 7, lines 16-60.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 2, 3, 6, 11, 12, 14, 15, 18, 19, 25, 26, 28, 29, 30, 31, and 32,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '483 as applied to above claims, in further view of Naveh et al., U.S. Patent No. 6,466,984 (hereinafter '984).

As to dependent claims 2, the following is not taught in '483 "wherein said regulating the activities comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria that are conditioned on said running state" however '984 teaches "For each flow generated by the application, this information is then used to map the application parameters attached to the flow into a concrete QoS decision and a signaling mechanism. For example, the process is notified by the application about the start of each flow with its parameters and this information is converted into QoS information usable by a network device. The simplest case is mapping one ACP into a DSCP value, as shown by block 710, and then setting a QoS value may be set by marking the flow packets using an appropriate operating system call to an existing QoSservice"" in col. 11, lies 44-56.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method of managing a network session taught in '483 to include a means filter the

packets of an application. One of ordinary skill in the art would have been motivated to perform such a modification because a need exits to integrate applications into a policy see '984 (col. 5, lines 12 et seq.). "Thus, there is a need for a mechanism that integrates application into a policy-based networking system, and enables applications to participate in deciding how to apply a particular QoS to a traffic flow generated by the application".

As to dependent claim 3, "wherein the rejection criteria include the predetermined configuration information" is shown in '984 col. 11, lines 3-17 "In block 704, policies are established based on the ACPs that are registered in association with the application".

As to dependent claims 6, "wherein regulating the activities comprises: providing a session layer adapted to reject unauthorized data packets based on context information; and providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies" is disclosed in '984 col. 11, lines 45-64.

As to dependent claims 11, 12, 14, and 15, these claims contain substantially similar subject matter as claims 2, 3, and 6 above; therefore they are rejected along the same rationale.

As to dependent claim 18, "further comprising a network stack" is taught in '984 col. 7, lines 48-60.

As to dependent claim 19, "wherein the network stack comprises: a policy engine connected to the first device; a policy store connected to the policy engine; a socket interceptor connected to the policy engine; and a packet guard connected to the policy engine" is shown in '984 col. 5, lines 19-67 "The method involves creating one or more mappings, each mapping representing an abstract policy ... The mappings are converted into one

or more settings of the network device, which enforces the policy in response to receiving traffic from the application program that matches the traffic flow type. One feature of this embodiment is that creating and storing one or more mappings comprises registering one or more application codepoints, which are associated with traffic flow types".

As to dependent claim 25, "wherein said remote system includes a network stack, and wherein said regulating activities comprises reconfiguring the network stack to control filtering of network packets, based on said policies and said running state" is disclosed in '984 col. 7, lines 16-60.

As to dependent claim 26, "wherein said policies include information about authorized kinds of information when certain applications are running, and said regulating activities comprises determining if a specified application is running, allowing a specified kind of network packet to pass only when said specified application is running, and blocking said specified kind of network packet from passing when said specified application is not running" is taught in '984 col. 15, lines 15-58 "FIG. 5 is a block diagram of a portion of a Repository that contains a Directory Schema 500. The Directory Schema 500 may represent the topology of a managed network or other directory information useful in network management .... Examples of servies include delay, guaranteed bandwidth a queuing type on a router interface, etcl. The services in the list also define signaling mechanisms that may be used for accessing the service".

As to dependent claims 28 and 29, these claims are substantially similar to claim 26 above and are rejected along the same rationale.

As to independent claim 30, "A method, comprising: establishing a virtual private network (VPN) session between a primary computing system and a remote computing system includes a security policy engine, and wherein the primary computing system includes a security policy engine" is taught in '483 col. 3, lines 29-60 "The forgoing objective is achieved by the system method and program product of the present invention in which a Virtual Private Network (VPN) is defined by the sum of a plurality of policy segments";

"and wherein the remote computing system includes a network stack" is shown in '984 col. 7, lines 48-60 "Communication facility 228 preferably includes one or more software libraries for implements a communication protocol stack"

"transmitting information indicative of security parameters from the primary computing system to the remote computing system using the security policy engine" is disclosed in 483 col. 5, lines 23-55 "In the preferred embodiment, a policy database is loaded or copied to a network device. FIG. 3 illustrates how a set of policies for a specific device are logically stored. It may have been downloaded from a server, provided by a device configuration application or entered from the network device's command line interface".

"configuring the network stack based on the information indicative of security parameters" is taught in '984 col. 9, lines 18-55 "A Schema stored in the Repository provides an integration point and a common information model for communication between Application 608 and Policy Server";

"subsequently running a particular application program on the remote computing system; selecting information indicative of updated security parameters based on a running state of the particular application program and dynamically reconfiguring the network

stack based on the information indicative of the updated security parameters" is shown in '984 col. 15, lines 15-55 "As shown in RIG. 5, Root node 502 is coupled to a plurality of Application nodes 504A, 504B, 504C. There may be any number of Application nodes. Each Application node represent a particular application program that is used in the managed network ... Each Policy Statement terminates in an Action. For example, Condition nodes 506A, 506B terminate at Action node 510. Each Action node represents an action to apply to network devices when an associated application generates a traffic flow such that the Policy Statement evaluates to TRUE".

As to dependent claim 31, "wherein the primary computing system is a corporate local area network (LAN)" is disclosed in '984 col. 7, lines 18-31 "An embodiment of the invention is used in the context of a network. FIG. 2 is a block diagram of a computer network 200 that includes a plurality of local area networks 202, 204, 206 interconnected by a plurality of intermediate network devices 208, 210. A plurality of network end stations, such as end station 212 and print server 214, are coupled to the LANs. The network further includes at least one policy server 216 that may be coupled to a repository 218 and to a network administrator station 220. A server suitable for use as policy server 216 is any Windows NT.RTM. or UNIX workstation or similar computer platform. Network 200 also includes at least one host or server 222 configured in accordance with the present invention"

As to dependent claim 32 "wherein the remote primary computing system is a remote home network" is taught in '984 col. 16 line 63 through col. 17, line 10 "Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor 804 for execution. For example, the instructions may initially be

carried on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system 800 can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal. An infra-red detector can receive the data carried in the infra-red signal and appropriate circuitry can place the data on bus 802. Bus 802 carries the data to main memory 806, from which processor 804 retrieves and executes the instructions. The instructions received by main memory 806 may optionally be stored on storage device 810 either before or after execution by processor 804"

9. **Claims 8, 16, and 20,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '483 as applied to above claims, in further view of Rothermel et al. U.S. Patent No. 6,678,827 (hereinafter '827).

As to dependent claim 8, the following is not taught in '483 **"further comprising: detecting data packets from the regulated activities; and rejecting the data packets from the regulated activities"** however '827 teaches "The routine begin a t step 705 where the NSD executes an initial boot program that loads the software to be executed by the NSD. After the software is loaded, the routine continues to step 710 to load various NSD-specific network packet filer rules that will be used to implement the specific security policy for the NSD ... the subroutine continues to step 820 to determine a default action to be taken for the packets. A variety of types of default actions can be used, including denying passage of all packets that are not explicitly approved" in col. 14, line 60 through col. 15, line 52.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method of managing a network session taught in '483 to include a means reject packets from regulated activities. One of ordinary skill in the art would have been motivated to perform such a modification because the progresses in technology create a need exits to mange confidential information see '827 (col. 1, lines 13 et seq.). "As computer systems and other network devices (e.g., printers, modems, and scanners) have become increasingly interconnected, it is increasingly important to protect sensitive information".

As to dependent claim 16, this claim contains substantially similar subject matter as claim 8; therefore it is rejected along similar rationale.

As to dependent claim 20, "the first device further comprising instruction to monitor the system for the intervening process" is taught in '827 col. 15, lines 3-7.

10. **Claims 27, 33 and 34,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '483 as applied to above claims, in further view of '984 in further view of '827.

As to dependent claim 27, the following is not taught in the combination of '483 and '984 **"wherein said specified application is a word processing program, and said kind of network packet is word processing data"** however '827 teaches "In addition, events of interest which trigger the logging of network security information or the notification of some entity can be defined and identified in a variety of ways, such as any packets to or from a particular device or a device in a particular class of devices, any packets for which a specific action are taken (e.g., deny passage), any packets containing contents of interest (e.g., particular words or an attached file of a particular type), any packets corresponding to a particular type of network service (e.g., HTTP requests), etc. Finally, a variety of means for providing security to

information being transmitted over a non-secure network can be utilized, including symmetric keys, asymmetric keys, passwords, etc.)" in col. 17, lines 10-22.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method of managing a network session and with a means to filter packets taught in '483 and '984 to include a means reject packets from regulated activities. One of ordinary skill in the art would have been motivated to perform such a modification because the progresses in technology create a need exits to mange confidential information see '827 (col. 1, lines 13 et seq.). "As computer systems and other network devices (e.g., printers, modems, and scanners) have become increasingly interconnected, it is increasingly important to protect sensitive information".

As to dependent claim 33, "wherein the particular application program is a word processing program and wherein when the running state of the work processing program indicates that the word processing program is not running, the information indicative of security parameters causes the remote computing system to block word processing packets received at the remote computing system" is shown in '827 col. 17, lines 10-22.

As to dependent claim 34, "wherein the particular application program is a word processing program, and wherein when the running state of the word processing program indicates that the word processing program is running, the information indicative of updated security parameters causes the remote computing system to not block word processing packets received at the remote computing system" is disclosed in '827 col. 17, lines 10-22

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
09 November 2004

Andrew Caldwell
Andrew Caldwell